Judge Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	NO. CR15-5351 RJB UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, S. Kate Vaughan, Assistant United States Attorney for said District, and Keith A. Becker, Trial Attorney, hereby files this response to Defendant's Motion to Suppress Evidence and Statements.

The defendant, Jay Michaud ("Michaud"), filed a motion to suppress evidence obtained via three court-authorized search warrants issued upon findings of probable cause by three neutral and detached magistrates, and of a Mirandized statement to law enforcement, alleging that the first of those search warrants was improperly issued. He does not challenge any of the assertions in any of the warrants. Rather, Michaud, a teacher with Vancouver Public Schools, contends that his use of a Tor-network-based child pornography website deprived any court of jurisdiction to issue a warrant to identify

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

him – an argument that, if accepted by this Court, could create an insurmountable legal barrier to protecting the children who are harmed by massive criminal enterprises like the targeted site. Thankfully, his contention is wrong. The issuance of the challenged warrant complied with Fed. R. Crim. P. 41 and the Fourth Amendment, and was amply supported by probable cause to investigate the registered users of a massive child pornography website whose users, including Michaud, deployed advanced technological measures to hide their identity and location while they exploited children. Moreover, suppression would be particularly inappropriate here, where law enforcement officers acted reasonably and in good-faith reliance upon the issuance of warrants. Accordingly, for the reasons set forth more fully below, the United States requests that this Court deny the motion to suppress.

I. INTRODUCTION

The charges in this case arise from an investigation into a global online forum, referenced herein as "Website A," through which registered users like the defendant regularly advertised, distributed and accessed illegal child pornography.[1] The scale of child sexual exploitation on the site was massive –more than 150,000 total members collectively created and viewed tens of thousands of postings related to child pornography. Images and videos advertised, distributed and accessed through the site were highly categorized according to gender and age of victims portrayed – including "jailbait," "pre-teen" and "toddlers" – as well as the type of sexual activity depicted – including hardcore ("HC") and softcore ("SC"). The most postings (more than 20,000) occurred within a sub-section for "Pre-teen" videos dubbed "Girls HC," that contained hardcore pornographic images of pre-teen girls. The site also included forums for discussion of matters pertinent to child sexual abuse, including methods and tactics

[1] In order to protect the security of the ongoing investigation, the actual name of the website was not disclosed in pertinent search warrant documents, but was alternately referenced as the "TARGET WEBSITE" or "Website A." It is referenced herein as "Website A."

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

offenders use to abuse children and avoid law enforcement detection. It did not advertise or distribute adult pornographic images.

"Website A" operated on the anonymous Tor network. Use of the Tor network masks the user's actual Internet Protocol ("IP") address,[2] which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers. [3] To access the Tor network, a user must install Tor software by downloading an add-on to the user's web browser or the free "Tor browser bundle" available at www.torproject.org.[4] Because of the way Tor routes communications through other computers, traditional IP-address-based identification techniques used by law enforcement agents investigating online crimes are not viable. When a Tor user accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node.

Within the Tor network itself, entire websites, such as "Website A," can be set up as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and replaced with a Tor-based web address, which is a series of 16 algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client

---

[2] An Internet Protocol address or "IP" address refers to a unique number used by a computer to access the Internet. IP addresses are assigned to residential Internet users by an Internet Service Provider ("ISP").

[3] Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is publicly available at www.torproject.org. The Tor network is a haven for criminal activity in general, and the online sexual exploitation of children in particular. *See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED MAGAZINE, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited November 13, 2015).

[4] Users may also access Tor through so-called "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

and operating in the Tor network. Unlike an open Internet website, it is not possible use public lookups to determine the IP address of a computer hosting a "hidden service."

A "hidden service" like "Website A" is also more difficult for users to find. Even after connecting to the Tor network, a user must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find "Website A," a user had to first obtain the web address for it from another source – such as from other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing a Tor website like "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity taking place on "Website A," investigators faced a tremendous challenge to identify site users who were sexually exploiting children. Open-Internet, non-Tor websites generally have user IP address logs that can be used to locate and identify the site's users. In such cases, after the lawful seizure of a website whose users were engaging in unlawful activity, law enforcement could review IP logs and determine the IP addresses of site users. Agents could then determine from publicly-available information which Internet Service Provider ("ISP") owned an IP address, and issue a subpoena to that ISP to determine the user to which the IP address was assigned at a pertinent date and time. However, because "Website A" was a Tor "hidden service," any such IP logs would contain only the IP address of the last computer through which a user communication was routed. That last computer is not that of the actual user who sent the communication, and it is not possible to trace such communications back through the Tor network to that user. Such IP address logs therefore could not be used to locate and identify users of "Website A." Accordingly, in order for law enforcement to attain the sort of information that would normally be available from public sources and through ordinary investigative

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

means, the offenders' use of the Tor network necessitated a particular investigative strategy.

Acting on a tip from a foreign law enforcement agency as well as information from its own investigation, the FBI determined that the computer server that hosted "Website A" was located at a web-hosting facility in North Carolina. In February of 2015, FBI agents apprehended the administrator of "Website A" and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of the site to go unidentified (and un-apprehended), the FBI allowed it to continue to operate at a government facility in the Eastern District of Virginia ("EDVA") during a brief two-week period between February 20, 2015, and March 4, 2015. During that brief period, the FBI obtained court authorizations from the United States District Court for the Eastern District of Virginia to (1) monitor site users' communications and (2) deploy a Network Investigative Technique ("NIT") on the site, in order to attempt to identify registered site users who were anonymously engaging in sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.[5]

As described in detail in the application for the warrant authorizing its use, the NIT consisted of computer instructions which, when downloaded (along with the other content of "Website A") by a registered user's computer, were designed to cause the user's computer to transmit a limited set of information – the computer's actual IP address and other computer-related information – that would assist in identifying the computer used to access "Website A" and its user. Ex. 1, pp. 23-27, ¶¶ 31-37. The search warrant authorization permitted that minimally-invasive technique to be deployed after a registered user logged into "Website A," which was located in EDVA, by entering a username and password. *Id.*, p. 24, ¶ 32; p. 23, Att. A.[6] IP address information

[5] The NIT search warrant, application, affidavit and return (No. 15-SW-89) are attached as Exhibit 1. The separate Title III application, affidavit and order are attached as Exhibit 5.

[6] The NIT affidavit explained that, in order to ensure technical feasibility and avoid detection of the technique by subjects of investigation, the FBI would deploy the technique more discretely against particular users, such as those

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

collected by the NIT, along with logs of activity on "Website A," was then used with further legal process to investigate "Website A" users.

At various points in his motion, Michaud, absent any factual or legal support or argument, inaccurately labels the government's court-authorized investigative technique as a "hacking." Mot. At 1, 8, 10. That is not the case. Even by dictionary definition, to hack involves gaining "unauthorized access to data" in a computer.[7] The federal statute under which what is colloquially known as computer hacking is commonly prosecuted – 18 U.S.C. § 1030 – criminalizes only the "unauthorized access" to a computer in certain defined circumstances and with particular stated intent. *Id*. The NIT, on the other hand, was a court-authorized investigative technique, whose deployment was supported by a showing of probable cause, that consisted of computer instructions designed only to cause the user's computer to transmit a limited set of information that would assist in identifying the computer used to access "Website A" and its user. Ex. 1, pp. 23-27, ¶¶ 31-37. The court-authorized NIT did not constitute "hacking" any more than a court-authorized search of a defendant's home, during which law enforcement seizes and removes evidence of a crime, constitutes burglary or theft. Michaud's use of such a loaded (and inaccurate) term is an obvious attempt to distract this Court's attention from the actual legal issues presented and invite a decision based upon something other than the pertinent facts and law. This Court should attach no weight to it whatsoever.

On July 9, 2015, law enforcement agents obtained from this District (Mag. J. David W. Christel) a search warrant for the defendant's home.[8] The warrant described "Website A" in detail and articulated that data obtained from logs on "Website A," court-authorized monitoring by law enforcement, and the court-authorized deployment of a NIT, had revealed that "Website A" user "Pewter" registered an account on "Website A"

---

who attained a higher status on the website by engaging in substantial activity, or in particular areas of the website, such as those with the most egregious examples of child pornography, which sub-forums were described in the affidavit. Ex. 1, pp 24-25, ¶ 32, n. 8.

[7] *See* Oxford Dictionaries Online, available at: http://www.oxforddictionaries.com/definition/english/hack (last visited November 16, 2015).

[8] The residential search warrant, application, and affidavit (No. 15-MJ-5111) are attached as Exhibit 2.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

on October 31, 2014 and spent 99 hours logged into the website between October 31, 2014, and March 2, 2015. Ex. 1, pp. 21-22, ¶¶ 25-26. Between February 20, 2015, and March 4, 2015, user "Pewter" viewed 187 message threads on the website, including threads with titles such as "10yo teen with anal front with his father," "Alicia 10 yo little girl loves adult sex (cum in mouth)," "7yo APRIL hj bj finger pencil in ass vib cum," "Lauri ~8yo 3 videos, tasting cum," and "Girl 12ish eats other girls/dirty talk." *Id.*, p. 22, ¶¶ 27-30. The warrant affidavit described specific child pornography "Pewter" accessed on March 2, 2015, which contained links to an image that depicted a prepubescent female being anally penetrated by the erect penis of an adult male. *Id.*, p. 23, ¶¶ 32-33. On February 28, 2015, user "Pewter," operating from IP address 73.164.163.63, accessed the post entitled "Girl 12ish eats other girls/dirty talk" in the section "Pre-teen Videos >> Girls HC." *Id.*, p. 22, ¶ 30. Information furnished by Comcast in response to an FBI subpoena tied the IP address collected by the NIT for "Pewter" to the Internet connection subscribed in his name at Michaud's then home. *Id.*, p. 23, ¶ 36. Further investigation determined that Michaud moved, as of May of 2015, to a new address that was the subject of the residential search warrant. *Id.*, pp. 23-26, ¶¶ 36-43.

On July 10, 2015, law enforcement officers executed a federal search warrant at Michaud's residence in Vancouver, WA. Agents located a thumb drive that was later determined to contain over 2,400 images of child pornography, including those depicting the anal rape of an infant and a toddler-aged child, and a 20-page manual entitled "The Jazz Guide: How to Have Sex With Very Young Girls . . . Safely." Ex. 4, p. 9, ¶ 31. Also on July 10, 2015, the defendant gave a brief, audio-recorded statement to law enforcement agents after being advised of his Miranda rights. He admitted to living alone and provided a password to his phone. After the interview, Michaud was arrested and charged by complaint with possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4) and (b)(2). A cell phone on the defendant's person was seized incident to his July 10, 2015 arrest. On August 11, 2015, officers obtained from this District (Mag.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

J. Karen Strombom) a warrant to search that phone, on which additional child pornography was located.[9]

On July 23, 2015, Michaud was indicted for receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4) and (b)(2). On October 16, 2015, the defendant filed a motion to suppress the NIT warrant and all information seized pursuant to it, including evidence obtained via execution of the residential search warrant and the defendant's post-Miranda statement to law enforcement.[10]

II. ARGUMENT

Michaud raises two unpersuasive arguments in his motion: that the issuance of the NIT warrant violated Rule 41 and that the defendant was not properly provided notice. On those purported bases, Michaud contends that evidence seized pursuant to that warrant and any related fruits should be suppressed. His arguments are without merit.

A. Summary of Argument

Michaud's argument for suppression based on a purported violation of the geographic limitations of Rule 41 fails for multiple reasons. Consistent with Rule 41, the NIT warrant was issued by a neutral and detached magistrate in the district where the website operated during the period of authorization, into which registered users – including Michaud – communicated while accessing the website, and in which the NIT was deployed. The Title III order for Michaud's communications with "Website A" also provided authority to obtain Michaud's IP address. And even if neither the NIT warrant nor the Title III order had provided authority for use of the NIT, its use would have been justified based on exigent circumstances pertaining to the ongoing exploitation and abuse of children and suspect offenders' use of anonymizing technology. Michaud's argument regarding delayed notice also fails, because the issuing Court authorized and extended delayed notice and Michaud was provided notice within the Court-authorized time frame.

---

[9] The search warrant, application, and affidavit (No. 15-5136) are attached as Exhibit 3.

[10] The defendant's motion to suppress does not make reference to the warrant to search the cell phone or its fruits.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The NIT warrant further satisfies the Fourth Amendment because it was issued based on a detailed, 31-page affidavit that amply articulated probable cause to deploy the NIT to registered users of a website dedicated to the advertisement and distribution of child pornography, and which described with particularity exactly what information would be collected through the NIT – IP address and other computer-related information – and how that information would assist with identifying site users and computers used to access the site. The affidavit accordingly established a more than fair probability that evidence of a crime – *i.e.*, of the identity of perpetrators – would be found via issuance of the warrant.

In any event, while neither the asserted violation of Rule 41 nor any of the defendant's other arguments warrant suppression, law enforcement acted at all times in good-faith reliance upon warrants issued upon findings of probable cause by neutral and detached magistrates in two different U.S. Districts. The extreme remedy of suppression is not justified where, as here, law enforcement diligently sought and received judicial approval to deploy an investigative technique necessitated by suspects' use of anonymizing technology to criminally exploit children.

B. The Warrant was Issued Consistent With Rule 41 and the Fourth Amendment

Michaud makes no substantive argument that the NIT warrant did not comply with the Fourth Amendment. Instead, he argues for suppression based on a purported violation of the geographic limitations of Rule 41. His argument fails for multiple reasons. First, the NIT warrant was consistent with Rule 41. Second, the Title III order for Michaud's communications with "Website A" also provided authority to obtain his IP address. Third, if neither the NIT warrant nor the Title III order provided authority for the NIT, its use would be justified based on exigent circumstances. Finally, even if the NIT warrant did violate Rule 41, suppression is not an appropriate remedy.

It is important to make clear the ramifications of Michaud's Rule 41 argument. When the government sought the NIT warrant, Michaud and thousands of others were

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

using "Website A" to access and share child pornography. The site was designed to hide the identity and location of its users, so the government had no way to know where Michaud was without first using the NIT authorized by the warrant. Thus, Michaud does not argue that the government should have sought its warrant elsewhere, or that the government should have more scrupulously followed any of the procedures of Rule 41 for obtaining or executing the warrant. Instead, Michaud is arguing that his use of the Tor hidden service deprived any court of jurisdiction to issue a warrant to identify him. If Michaud were correct, use of a Tor hidden service could potentially create an insurmountable legal barrier to protecting the children who are harmed by massive criminal enterprises like the targeted hidden service. Fortunately, Michaud is wrong.

Courts interpret Rule 41 broadly to allow searches consistent with the Fourth Amendment. For example, in *United States v. New York Telephone Co.*, 434 U.S. 159 (1977), the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" at that time did not include information and that Rule 41 required that a search be conducted within 10 days. *See id.* at 169 & n.16. The Court held that Rule 41 "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause," and it bolstered its conclusion by reliance on Rule 57(b), which provided that "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *Id.* at 169-70.[11] Similarly, in *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992), the Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. Moreover, as the Seventh Circuit recognized, denying courts the authority to issue warrants for searches consistent with the Fourth Amendment would encourage warrantless searches, as such searches could be justified

[11] Rule 57(b) now provides: "A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

based on exigency: "holding that federal courts have no power to issue warrants authorizing [an investigative technique] might . . . simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment." *United States v. Torres*, 751 F.2d 875, 880 (1984) (upholding video surveillance warrant). Based on the reasoning of these cases, this Court should reject Michaud's argument that Rule 41 should be interpreted narrowly to prohibit the use of search warrants to investigate those who use Tor to hide the location of their criminal activities.

In any event, the government did not violate Rule 41. Rule 41(b) is flexible enough to allow the issuance of warrants to investigate Tor hidden services.[12] In fact, three separate provisions of Rule 41(b) support issuance of the NIT warrant.

First, Rule 41(b)(2) allows a magistrate judge "to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Here, the warrant authorized use of the NIT (a set of computer instructions) located on a server in EDVA when the warrant was issued. Ex. 1, pp. 22-23, 24 ¶¶ 30, 33. As Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information," the NIT constituted property located in EDVA when the warrant was issued. Moreover, the NIT was deployed only to registered users of "Website A" who logged into the website, located in EDVA, with a username and password. *Id.*, Att. A. Each of those users – including Michaud – accordingly reached into EDVA's jurisdiction

---

[12] In order to eliminate any ambiguity on this issue, the Advisory Committee on Criminal Rules has endorsed an amendment to Rule 41 to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." *See* Advisory Committee on Rules of Criminal Rules, May 2015 Agenda, at 107-08 (available at http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books). The proposed rule was approved by the Advisory Committee on the Criminal Rules in March 2015 and the Standing Committee in May 2015. It is now pending further review before the U.S. Judicial Conference. *See* http://www.uscourts.gov/rules-policies/pending-rules-amendments.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

to access the site (and the child pornography therein). Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT outside of EDVA.

Similarly, Rule 41(b)(4) specifies that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). In a physical tracking device case, investigators might obtain a warrant to install within the district a tracking device in a container holding contraband, and investigators might then determine the location of the container after targets of the investigation carry the container outside the district. In this case, the NIT functioned in a similar manner, except in the Internet context. Investigators installed the NIT in EDVA on the server that hosted "Website A." When Michaud logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information from Michaud's computer back to law enforcement. Although this network information was not itself location information, investigators subsequently used this network information to identify and locate Michaud. Thus, even if Rule 41(b)(2) did not provide authority to issue the warrant, Rule 41(b)(4) did so.

Furthermore, the EDVA warrant was issued by a judge in the district with the strongest known connection to the search: Michaud retrieved the NIT from a server in EDVA, and the NIT sent his network information back to a server in that district. The magistrate judge had authority under Rule 41(b)(1) to authorize a search warrant for "property located within the district." In addition, Michaud's use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in. In this circumstance, it was reasonable for the EDVA magistrate judge to issue the warrant. Interpreting Rule 41 to allow the issuance of warrants like the EDVA warrant does not risk significant abuse because, as with all warrants, the manner of execution "is subject to later judicial review as to its

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). For these reasons, this Court should conclude that issuance of the warrant did not violate Rule 41.

Michaud cites a single magistrate judge's opinion holding that Rule 41(b) does not authorize issuance of a warrant for use of a different (and significantly more invasive) NIT than the one used in this case. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). But that court did not fully consider the arguments here for the issuance of the warrant, let alone the arguments why suppression would be inappropriate after such a warrant was issued by a neutral and detached magistrate. Furthermore, to the government's knowledge, in every other matter involving an application for a search warrant to identify a person hiding his identity and location using Internet anonymizing techniques, the judge has issued the warrant. *See, e.g., United States v. Cottom, et. al.*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #122, Attachment 1; Doc. #123, Attachment 1) (2 separate NIT search warrants), (Doc #155) (denying suppression motion); *In re Search of NIT for Email Address texas.slayer@yahoo.com*, No. 12-sw-5685 (D. Col. October 9, 2012) (Doc #1) (search warrants); *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government*, No. 07-mj-5114 (W.D. Wash. June 12, 2007), *available at* http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf.

Moreover, the reasoning of the Texas magistrate judge's decision does not apply to the use of the NIT in this case. That court correctly found it "plausible" that the NIT fell within the definition of a tracking device. 958 F. Supp. 2d at 758. Nevertheless, the court held that Rule 41(b)(4) did not apply because there was no showing that the installation of the NIT software would be within its district. *See id*. That was not the case here: installation of the NIT within the meaning of Rule 41(b)(4) took place on the server in EDVA. As the analogy to physical tracking devices demonstrates, the government "installs" the NIT within the meaning of Rule 41(b)(4) when it adds the NIT

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

to computer code on a computer in the issuing court's district. Michaud's subsequent retrieval of the NIT and its collection of information from his computer constituted "use of the device" for purposes of Rule 41(b)(4), regardless of whether that process of collection included "installation" on Michaud's computer.

The Rule 41 warrant is not the only court order providing authority to obtain Michaud's true IP address, however – the Title III order also provided such authority. The Ninth Circuit has held that when the government obtains a Title III order to intercept contents of communications, it may also collect associated non-content information. *See United States v. Kail*, 612 F.2d 443, 448 (9th Cir. 1979). That is what the government did here: it used the NIT to determine the true IP address associated with communications that the government was authorized to intercept pursuant to a Title III order.

In *Kail*, a pre-pen register statute case, the government obtained a wiretap order, but it did not obtain separate authorization for the pen register it installed to collect associated dialed phone number information. As the Ninth Circuit explained, "[b]ecause pen registers do not intercept the contents of communications, they are not within the scope of Title III." *Kail*, 612 F.2d at 448. The court held, however, that obtaining a wiretap order was sufficient authorization for the pen register: "once a valid wiretap order has been issued, as here, there need not be separate authorization for the pen register. . . . If, as defendants argue, the Government must support the use of the pen register by a showing of probable cause that showing is met by satisfying the probable cause requirements for obtaining the wiretap." *Id.*

In this case, the government obtained a Title III order that authorized it to intercept Michaud's communications with "Website A." Ex. 5. Order, p. 2-3. The district court in EDVA had jurisdiction to issue this order, as the order authorized interception of communications with a server located in that district. *See* 18 U.S.C. § 2518(3). The order authorized the government "to intercept electronic communications of the TARGET SUBJECTS occurring over the TARGET FACILITIES, until such electronic communications are intercepted that fully reveal: . . . the location and identity of

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

computers used to further the offenses." *Id*. at 3. Michaud's communications with "Website A" fell within the scope of this authorization.

Thus, under the holding of *Kail* that "once a valid wiretap order has been issued, as here, there need not be separate authorization for the pen register," the Title III order provided appropriate authority for the government to collect non-content information associated with the intercepted communications, including Michaud's true IP address. The Ninth Circuit has held that IP address information in the Internet context is analogous to dialed number information in the telephone context. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007). Although IP address information is typically collected without a warrant at all, *see id.* at 510-511, the government here had authority to collect it both under the Title III order and the Rule 41 warrant. As in *Kail*, "[i]f . . . the Government must support the use of the pen register by a showing of probable cause that showing is met by satisfying the probable cause requirements for obtaining the wiretap." Indeed, the government explained to the issuing district court in its Title III affidavit that it planned to use the NIT to determine the true IP address of website users. *Id.*, Affidavit, p. 31. The government also stated that it planned to obtain additional authorization to use the NIT (which it did), but under *Kail*, additional authorization was not essential. Because the Title III order provided sufficient authority to collect Michaud's true IP address when he accessed "Website A," his motion to suppress should be denied.

Even if Michaud were correct that Rule 41 did not allow the government to obtain a warrant for use of the NIT, and if the Title III order did not provide authorization either, then the use of the NIT would nevertheless still be reasonable under the Fourth Amendment. The Supreme Court has recognized that the presumption that warrantless searches are unreasonable "may be overcome in some circumstances because '[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). "One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a]

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

warrantless search is objectively reasonable under the Fourth Amendment." *Id.* (internal quotation marks omitted). The Ninth Circuit has defined exigent circumstances as "those circumstances that would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *United States v. Martinez*, 406 F.3d 1160, 1164 (9th Cir. 2005) (quoting *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir.1984) (*en banc*) (abrogated on other grounds)). Courts must evaluate "the totality of the circumstances" to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 59 (2013).

Here, if the government could not obtain a warrant for use of the NIT, use of the NIT was justified by exigency. There was a compelling need to use the NIT: "Website A" enabled ongoing sexual abuse and exploitation of children on a massive scale, and use of the NIT was necessary both to stop the abuse and exploitation and to identify and apprehend the abusers. The information it collected was fleeting – if law enforcement had not collected IP address information at the time of user communications with "Website A," then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information. Accordingly, if the warrant could not be issued, then no warrant could have been obtained in a reasonable amount of time to identify perpetrators. *See United States v. Struckman*, 603 F.3d 731, 738 (9th Cir. 2010) (stating that to invoke the exigent circumstances exception, "the government must . . . show that a warrant could not have been obtained in time").

Moreover, the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information: it only authorized collection of IP address information and other basic identifiers for site users. An IP address belongs to an ISP, not Michaud, and the Ninth Circuit has held that a defendant lacks a reasonable expectation of privacy in IP addresses. *Forrester*, 512 F.3d at 510. Before proceeding with a more invasive

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

entry and search of Michaud's home and electronic devices, the government obtained a Rule 41 warrant issued in this district.

In sum, the NIT warrant and the Title III order provided authority for use of the NIT, and it is preferable that the government use warrants (as here) to investigate large criminal enterprises like "Website A." Criminals use anonymizing technologies like Tor to perpetrate crimes should not place them beyond the reach of law enforcement (or courts). But even if no court had authority to issue a warrant to deploy a NIT to investigate "Website A" users, its use was nonetheless reasonable under the Fourth Amendment.

C. Suppression is Neither Required Nor Reasonable in this Case

Assuming *arguendo* that the warrant was somehow deficient under Rule 41, suppression is neither required by law nor reasonable under the circumstances. "Rule 41 violations fall into two categories: fundamental errors and mere technical errors." *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). "Fundamental errors are those that result in clear constitutional violations." *Id*. By contrast, technical errors may only trigger suppression upon a proper showing of prejudice or "deliberate disregard" for Rule 41. *Id*.[13]

Suppression is a disfavored outcome in this circuit, even in cases presenting constitutional violations. *See, e.g.*, *Negrete-Gonzales*, 966 F.2d at 1283. "[W]e have repeatedly held – and have been instructed by the Supreme Court – that suppression is rarely the proper remedy for a Rule 41 violation." *United States v. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006). "Because the exclusionary rule tends to exclude evidence of high reliability, the suppression sanction should only be applied when necessary and not in any automatic manner." *United States v. Luk*, 859 F.2d 667, 671 (9th Cir. 1988) (affirming denial of suppression motion despite a technical violation of Rule 41).

[13] Michaud argues that all three bases apply, though he casts the alleged Rule 41 violations as "of constitutional magnitude" and "not mere technical violations." Mot. at 15, 16. While his argument appears cabined to just presenting a fundamental violation, the Government will respond to all of his arguments for sake of completeness.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Whether exclusion is warranted "must be evaluated realistically and pragmatically on a case-by-case basis." *Id*. (*quoting United States v. Vasser*, 648 F.2d 507, 510 n.2 (9th Cir. 1981), *cert. denied*, 450 U.S. 928 (1981)).

None of the three bases Michaud alleges warrant suppression stand up to scrutiny. He argues that the alleged violation of Rule 41's jurisdictional limitations "is of constitutional magnitude because it did not involve mere ministerial violations of the rule." Mot. at 14. But he offers no credible analysis of how use of the NIT represented a "clear constitutional violation." *See United States v. Johnson*, 660 F.2d 749, 753 (9th Cir. 1981) (requiring a showing that the search was "unconstitutional under traditional fourth amendment standards"). That is because none occurred. The Ninth Circuit has made clear that a "paradigmatic example" of a constitutional violation is where *no* warrant is sought. *Luk*, 859 F.2d at 673 (*citing United States v. Alvarez*, 810 F.2d 879 (9th Cir 1987)). In *Alvarez*, the court reversed the defendant's conviction because the district court did not order suppression after the Government arrested the defendant in a non-public place without a warrant despite having sufficient time to obtain one telephonically pursuant to then-Rule 41(c)(2). 859 F.2d at 882-84. That is clearly not the case here. Also, courts have repeatedly found that "a warrant issued by an unauthorized judge" – which Michaud appears to consider the EDVA magistrate judge to be – is not a fundamental or constitutional violation. *Luk*, 859 F.2d at 673 (*citing United States v. Ritter*, 752 F.2d 435 (9th Cir. 1985), *Johnson*, 660 F.2d 749, *United States v. Comstock*, 805 F.2d 1194 (5th Cir. 1986)).

Furthermore, the search and seizure here complied with the Fourth Amendment. The Fourth Amendment states that search warrants may be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. As the Supreme Court has emphasized, this language "require[s] only three things": a warrant must be issued by a neutral magistrate, it must be based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

a particular offense," and it must satisfy the particularity requirement. *Dalia*, 441 U.S. at 255. The NIT warrant satisfies these requirements. As described *infra*, the NIT warrant affidavit amply supported the magistrate's finding of probable cause. Ex. 1, pp. 10-23, ¶¶ 6-30. It further described the NIT, how it would be deployed against users who logged into the target website, and the limited, non-content information that would be seized as a result of the NIT's deployment. *Id*. at pp. 23-27, ¶¶ 31-37, Atts. A and B.

The Government's actions here were also reasonable under the circumstances. Law enforcement has a substantial interest in identifying users of a massive website trafficking in child pornography. The court-authorized use of the NIT was driven by the Tor-based technology Michaud and other offenders under investigation used to exploit children, which made it impossible for investigators to know where he was located without first using the NIT. *Id*., p. 23-24, ¶ 31. The individual privacy interests here were extremely limited, due to the minimally invasive nature of the NIT search and its focus on IP address information over which Michaud lacks a reasonable expectation of privacy. *See Forrester*, 512 F.3d 500 (Internet users have no expectation of privacy in the IP addresses of the websites they visit); *see also United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers."). Courts must weigh those privacy interests against "the needs of law enforcement," such as the "need for flexibility that allows police to do their job effectively." *United States v. Martinez-Garcia*, 397 F.3d 1205, 1211 (9th Cir. 2005). The very fact the government sought and obtained a warrant from a neutral magistrate protected Michaud from an unreasonable search and seizure in violation of his constitutional rights. *See Alvarez*, 810 F.2d at 883 (interposing magistrate between law enforcement and target protects against unreasonable searches and seizures). Obtaining that warrant from a magistrate judge in the district where the website was hosted and where users like Michaud went to retrieve information from the website was eminently reasonable, particularly given the lack of available options. Moreover, the magistrate

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

judge did not fail in her duty to impartially evaluate the government's request, nor did the government fail to provide any pertinent information to the magistrate judge. The affidavit, for instance, expressly sought authorization to "cause an activating computer – *wherever located* – to send" certain information to a government-controlled computer, Ex. 1, p. 29, ¶ 46(a)(emphasis added), and it repeatedly noted that a primary purpose of the NIT was to "locate" website users. *Id.*, p. 23-25, ¶¶ 31-32, 34.

Michaud argues that he was prejudiced because, he claims, the search of his computer would not have occurred had the Government limited the NIT to just activating computers located in EDVA. *See* Mot. at 15. The actual import of his prejudice argument is that he believes he had a right to anonymously exploit children without being identified by law enforcement using court-authorized investigative methods. That is not the sort of claimed "prejudice" that should result in suppression. Having used Tor to shield his location from investigators, Michaud should not be permitted to wield it as a weapon against the Government's ability to ask a court to authorize a search to identify him. In any event, as noted *supra*, the government nonetheless could have proceeded with the NIT search without a warrant, due to the exigent circumstances created by Michaud's use of the Tor network to conceal his location and identity.

Even if the government knew the location of activating computers, Michaud still would not have been prejudiced. For instance, had Michaud not concealed his true location, the Government could have obtained a search warrant from a magistrate judge in this district. *See United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (rejecting claim of prejudice where law enforcement officer could have obtained warrant from a separate judicial officer); *Johnson*, 660 F.2d at 753 (same). Michaud's reliance on cases such as *United States v. Krueger* and *United States v. Glover* does not alter this. Those cases involved searches of a residence and a car whose precise physical location were known to be located outside of the magistrates' districts when the warrants were issued. *See Krueger*, 998 F. Supp. 2d 1032, 1034-35 (D. Kan. 2014); *Glover*, 736 F.3d 509, 510 (D.C. Cir. 2013). Appropriate warrants, it stands to reason, could have been

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

obtained from judges in the districts where the residence and car were located. Those courts did not consider the facts before this court – where: (1) the defendant deliberately concealed his location, effectively rendering it impossible to seek process in another district, (2) the search occurred only after the defendant entered the magistrate's district by logging onto a server in that district, and (3) the scope of the search was limited to IP address and basic computer-related information.

Michaud also alleges that suppression is appropriate because agents intentionally and deliberately disregarded Rule 41's jurisdictional limitations. *See* Mot. at 16. But the government's putative violation hardly rises to the level of "bad faith." *Luk*, 859 F.2d at 673 ("suppression is required for nonfundamental violations in bad faith"); *see also Williamson*, 439 F.3d at 1134 ("[o]ther cases have equated 'deliberate and intentional disregard' with 'bad faith.'"). As in *Luk*, the warrant request here was the product of a lengthy investigation by agents who, rather than attempting to avoid compliance with Rule 41, deliberately sought to satisfy the letter of Rule 41 by seeking a warrant in the district with the greatest known connection to the criminal activity. *See* 859 F.3d at 675 (describing investigation). There is no evidence that agents hid critical information from the magistrate judge, or otherwise prevented the magistrate from having all the necessary information. This case is hardly analogous to cases such as *United States v. Gantt*, where the Ninth Circuit affirmed suppression because agents deliberately and without justification failed to provide an individual with a copy of a warrant upon request during a search, in violation of Rule 41(d). 194 F.3d 987, 994-95 (1999). Rather, law enforcement reasonably concluded that under Rule 41, an EDVA judge could issue a warrant to install a NIT on a server in EDVA which would be activated only after individuals, whose true location they deliberatively concealed, voluntarily entered EDVA to access the server. Even if that conclusion was erroneous, such a misapprehension is not equivalent to "bad faith" and does not justify suppressing highly probative evidence that agents used to identify Michaud. *See Williamson*, 439 F.3d at 1134 ("where the agent executing the warrant is unaware of the Rule but acts in good faith in executing

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

what he or she believes to be the Rule, he or she has not acted in deliberate disregard of it; thus suppression is not appropriate").

Finally, even if the warrant was not authorized under Rule 41, the good faith exception applies. *See Leon*, 468 U.S. 897 (1984); *Negrete-Gonzales*, 966 F.2d at 1283 (applying good faith doctrine in the context of a Rule 41 violation). The Supreme Court has made clear that, "the exclusionary rule should not be applied when the officer conducting the search acted in objectively reasonable reliance on a warrant issued by a detached and neutral magistrate," even if that warrant "is subsequently determined to be invalid." *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). The analysis turns on whether there is "an *objectively reasonable* basis for [the agents'] mistaken belief that the warrant was valid." *Negrete-Gonzales*, 966 F.2d at 1283 (emphasis in original). Given the strong nexus between the criminal conduct here and EDVA, and the fact that Michaud and others obscured their true location using Tor, it was entirely reasonable to conclude that a judge in EDVA had authority to issue a valid search warrant under Rule 41. Moreover, once the magistrate signed the warrant after having been made aware of how the NIT would be implemented and its reach, the agents' reliance on that authority was objectively reasonable. *See Sheppard*, 468 U.S. at 989-90 ("we refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested").

Taken together, suppression here is clearly not warranted given that it is rarely appropriate and requires a careful, fact-specific, and pragmatic evaluation; the compelling need for law enforcement to identify users of this website; Michaud's actions to obscure his criminal activity and location from law enforcement; the review here by a neutral magistrate; and the extensive connections between EDVA and the criminal activity, including the fact that Michaud entered the district to access a child exploitation website.

D. Probable Cause Supported the Issuance of the NIT Search Warrant

The defendant does not challenge whether probable cause existed to issue the NIT warrant. Nor would any such argument be persuasive. The 31-page NIT search warrant

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

affidavit, sworn to by a veteran FBI agent with 19 years of federal law enforcement experience and specialized training and experience investigating the sexual exploitation of children, comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist law enforcement in identifying registered site users who were utilizing anonymizing technology to expose children to ongoing and pervasive sexual exploitation. Ex. 1, p. 1, ¶ 1.

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas v. United States*, 517 U.S. 690, 696 (1996). It is a fluid concept that focuses on "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (quotation marks omitted). The task of a judge evaluating a search warrant application "is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. Probable cause requires "only the probability, and not a prima facie showing, of criminal activity." *Gates*, 462 U.S. at 235. "Whether there is a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a 'commonsense, practical question,'" for which "[n]either certainty nor a preponderance of the evidence is required." *Gates*, 462 U.S. at 246; *see also United States v. Kelley*, 482 F.3d 1047, 1051-52 (9th Cir. 2007), and *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006). Indeed, "[f]inely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision." *Gates*, 462 U.S. at 235. The affidavit clearly established a fair probability that the use of the NIT would collect evidence of a crime.

As the NIT affidavit explained, users who wished to access "Website A" were required to register an account, accept registration terms and create a username and password before they could access the site. Ex. 1, p. 14-15, ¶¶ 12-14. Upon registration,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

all of the sections, forums, and sub-forums were observable. *Id*., p. 15, ¶ 14. The vast majority of those sections were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. *Id*., pp. 15-16, ¶14. The affidavit described, in graphic detail, particular child pornography that was available to all registered users of Website A, that depicted prepubescent females, males and toddlers, being subjected to sexual abuse and exploitation by adults. *Id*., pp. 17-18, ¶ 18. Although the affidavit clearly stated that "the entirety of [Website A was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id*. pp. 20-21, ¶ 27.

It is unlawful to access any computer disk – such as a website's computer server – with the intent to view child pornography, or to attempt to do so. 18 U.S.C. § 2252A(a)(5)(b). Accordingly, among other offenses, any suspect user of "Website A" who accessed the site, or attempted to, with that intent would be guilty of that crime. To that end, the veteran NIT affiant affirmatively articulated that there was "probable cause to believe that . . . any user who successfully accesse[d]" the website had, at a minimum, "knowingly accessed with intent to view child pornography, or attempted to do so." Ex. 1 p. 13, ¶ 10. He made that assessment in light of the "numerous affirmative steps" required for a user to find and access "Website A," which made it "extremely unlikely that any user could simply stumble upon" the site "without understanding its purpose and content." Ex. 1, p. 12-13, ¶ 10. The Ninth Circuit has repeatedly held that "a magistrate may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found," *United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990) (quoting *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987)), including in child pornography cases. *See, e.g., United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000) (finding affidavit that included statements based on affiant's training and experience regarding child pornography trafficking and storage provided substantial basis for probable cause determination).

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

The affiant's assessment (and, accordingly, the magistrate's reasonable reliance upon it) was overwhelmingly supported by information articulated within the warrant. "Website A" was no ordinary, run-of-the-mill website that any unknowing person could stumble upon, let alone access. Rather, because the website operated on Tor, a user first had to connect to Tor network and find the site, which required a user to obtain its lengthy, alphanumeric web address. Ex. 1, p. 12, ¶10. That user "might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location" – such as from a Tor "hidden service" page dedicated to pedophilia and child pornography, which contained a section with links to Tor hidden services that contain child pornography – including "Website A". *Id.* Moreover, upon arrival at the site's main page, before logging in, a user saw "to either side of the site name . . . two images depicting partially clothed prepubescent females with their legs spread apart." *Id.* 1, p. 13 ¶ 12. The text underneath those suggestive images of prepubescent girls – "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview" – indicated the site's dedication to image distribution. *Id.* 1, p. 13, ¶ 12.[14] The site's registration terms also contained numerous indications that the site pertained to illicit activity – repeatedly warning prospective users to be vigilant about their security and the potential of being identified. *Id.*, pp. 14-15, ¶ 13. The issuing magistrate could accordingly have reasonably drawn an inference that any user who successfully found "Website A" was aware of its purpose and content.

The full, documented content of the website, as described in the affidavit, made it evident that the site's primary purpose was to advertise and distribute child pornography. Courts have routinely held that membership to a child pornography website, even without specific evidence of suspect downloading child pornography, provides sufficient probable

[14] The affiant articulated that, [b]ased on [his] training and experience, [he] know[s] that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to the site and ".7z" refers to a preferred method of compressing large files or sets of files for distribution." Ex. 1, p. 13, ¶ 12.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

cause for a search warrant because of the commonsense, reasonable inference that someone who has taken the affirmative steps to become a member of such a website would have accessed, received or downloaded images from it. *See Gourde*, 440 F.3d at 1070 (finding sufficient probable cause for residential search where defendant paid for membership in a website that contained adult and child pornography; noting reasonable, common-sense inference that someone who paid for access for two months to a website that purveyed child pornography probably had viewed or downloaded such images onto his computer); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005) (finding probable cause where purpose of the e-group "girls12-16" was to distribute child pornography; noting "[i]t is common sense that an individual who joins such a site would more than likely download and possess such material"); *United States v. Shields*, 458 F.3d 269 (3rd Cir. 2006) (finding probable cause where defendant voluntarily registered with two e-groups devoted mainly to distributing and collecting child pornography and defendant used suggestive email address); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) ("[I]t is common sense that a person who voluntarily joins a [child pornography] group . . . , remains a member of the group for approximately a month without cancelling his subscription, and uses screen names that reflect his interest in child pornography, would download such pornography from the website and have it in his possession."); *United States v. Hutto*, 84 Fed. Appx 6 (10th Cir. 2003) (affidavit sufficient to show probable cause where defendant became a member of a group whose obvious purpose was to share child pornography, and the images were available to all group members); *but see United States v. Falso*, 544 F.3d 110 (2nd Cir. 2008) (suppressing evidence from residential search for lack of probable cause where defendant was never accused of actually gaining access to the website that contained child pornography, there was no evidence that the primary purpose of the website was collecting and sharing child pornography, and defendant was never said to have ever been

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

a member or subscriber of any child pornography site).[15] Here, like *Gourde*, the reasonable inference that the registered "Website A" users, at a minimum, accessed the site, or attempted to do so, with the intent to view child pornography easily meets the "fair probability" test.

E. The Government Provided Timely Notice of the Search Warrant

Michaud also contends that he was not provided timely notice of the execution of the NIT warrant. He is incorrect. The issuing magistrate authorized delayed notice, which was lawfully extended past the date on which the government provided Michaud with a copy of the warrant.

Rule 41 allows for the delay of any notice required by the rule "if the delay is authorized by statute." Fed R. Crim P. 41(f)(3). The NIT affidavit specifically requested that any notice due to be provided to the person from whom, or from whose premises, property was taken, be delayed pursuant to Fed. R. Crim. P. 41(f)(3) and 18 U.S.C. § 3103a. Ex. 1, pp. 27-28, ¶¶38-41; Warrant App. The Court granted the delayed notice request, checking the box on the warrant to commemorate a finding that "immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial)," and authorizing "the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized for 30 days." *Id*., Warrant.

Title 18 Section 3013a(c) permits the court to extend delayed notice for good cause shown. On April 3, 2015, June 30, 2015, and September 24, 2015, the U.S. District Court for EDVA granted 90-day extensions of delayed notice. Ex. 4. The September 24, 2015, extension runs until December 23, 2015. The defendant concedes that he was provided a copy of the NIT warrant, through discovery, as of August 19, 2014. Mot. at 17. Accordingly, any notice due was lawfully delayed and timely provided.

---

[15] All of those cases evaluated probable cause before 18 U.S.C. § 2252A(a)(5)(B) was amended to make it unlawful to knowingly access a computer disk with intent to view child pornography, compare 18 U.S.C. § 2252A(a)(5)(B)(effective July 27, 2006) with 18 U.S.C. § 2252A(a)(5)(B)(effective October 8, 2008), making this case even stronger in terms of probable cause.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

III. CONCLUSION

For all the foregoing reasons, the Court should deny Defendant's motion to suppress.

Dated this 16th day of November, 2015.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

s/ S. Kate Vaughan
S. KATE VAUGHAN
Assistant United States Attorney
700 Stewart Street, Suite 5200
Seattle, WA
Phone: (206) 553 7970
Fax: (206) 553 0882
E-mail: kate.vaughan@usdoj.gov

s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 16, 2015, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorneys of record for the defendant.

/s/ Rebecca Eaton

LISA CRABTREE
Legal Assistant
United States Attorney's Office
700 Stewart St., Suite 5220
Seattle, Washington 98101
Telephone: (206) 553-5127
Fax: (206) 553-0755
E-mail: rebecca.eaton@usdoj.gov